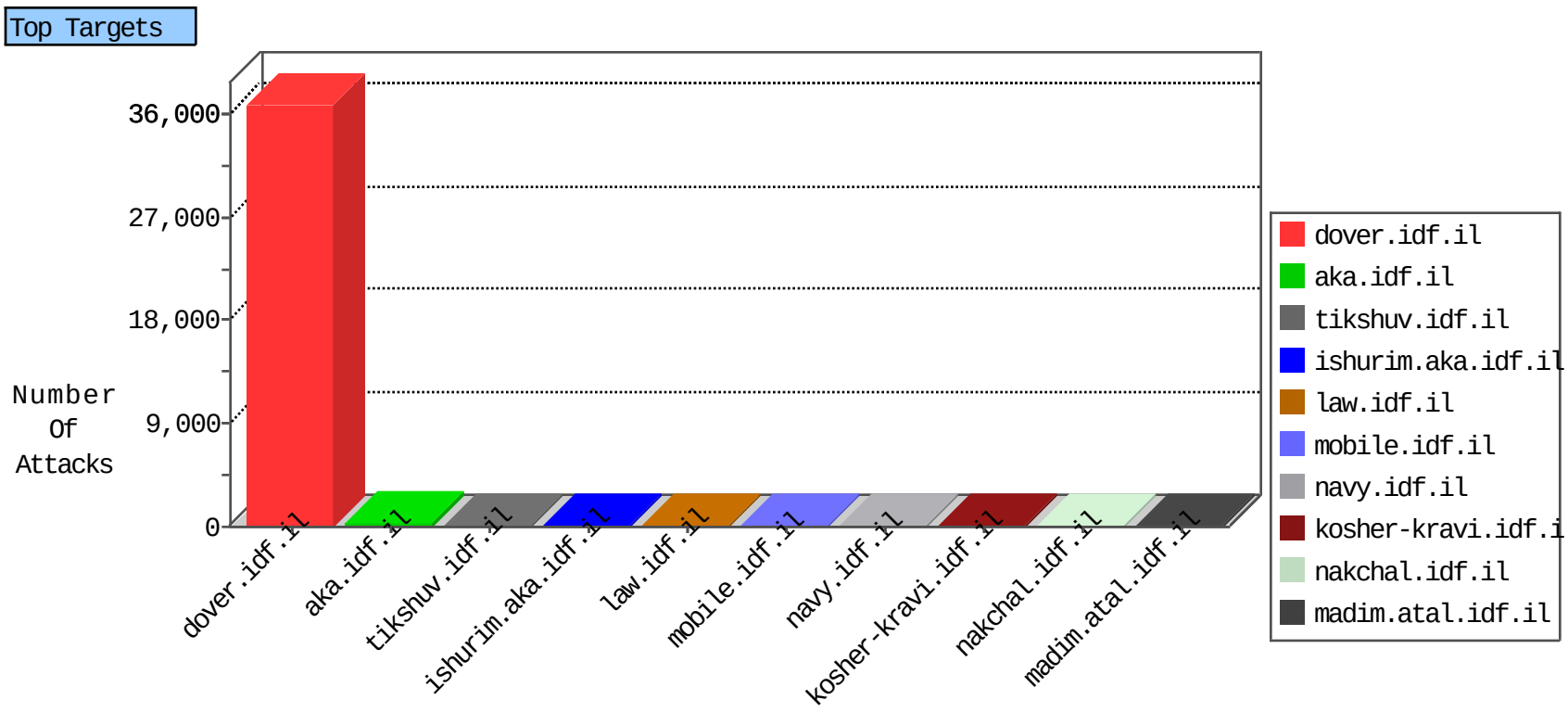
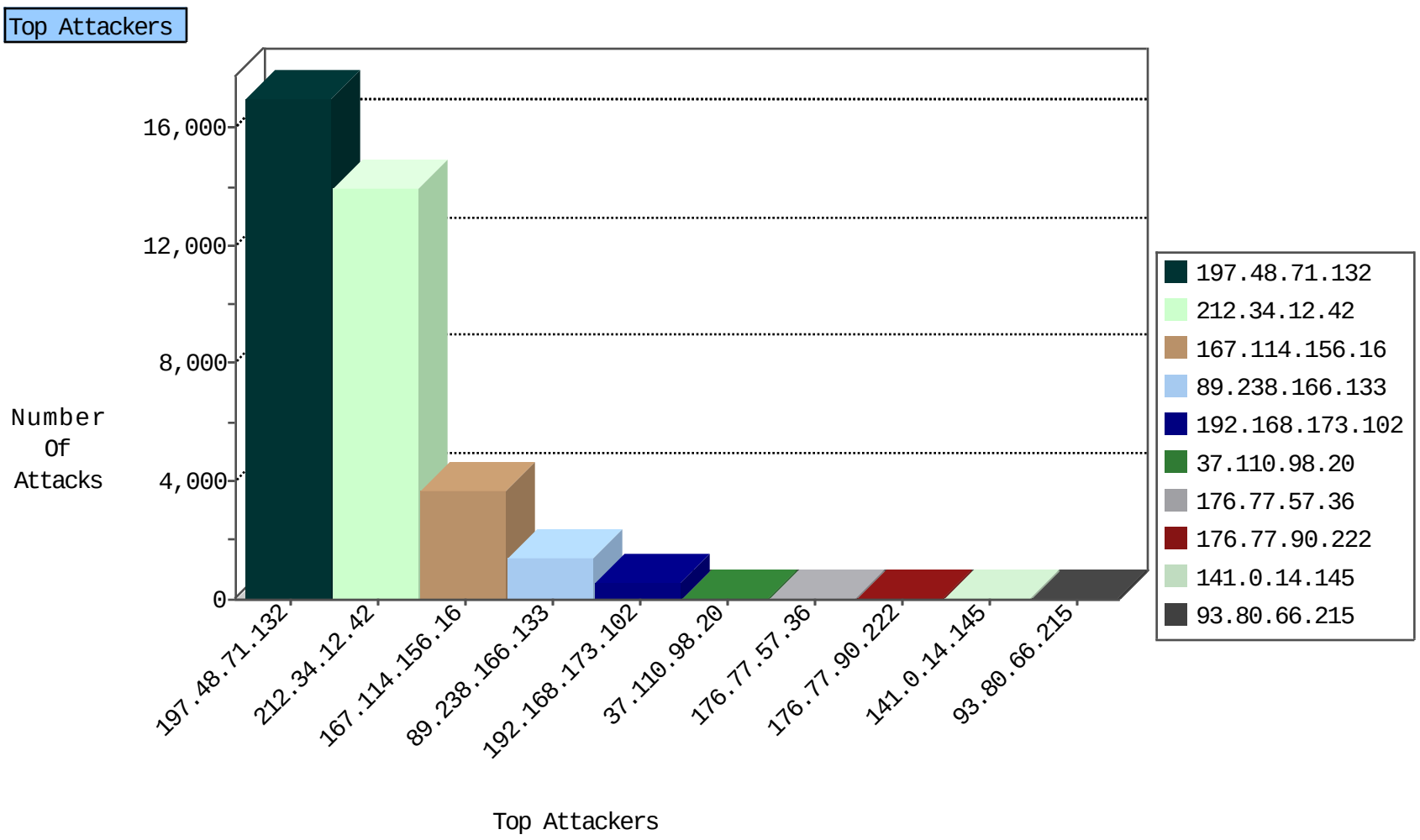
04-08-2016-01:08:24 to 04-08-2016-02:08:24

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-08-2016-01:08:24 to 04-08-2016-02:08:24

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	25484
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3709
89.238.166.133	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1394
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	694
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	91
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	34
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	29
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	10
41.68.43.187	Egypt	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
69.197.185.22	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
74.91.18.45	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
74.91.18.45	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
192.3.220.210	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
192.3.220.210	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
192.3.220.210	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
192.3.220.210	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

04-08-2016-01:08:24 to 04-08-2016-02:08:24

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-08-2016-01:08:24 to 04-08-2016-02:08:24

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.64.165	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
132.74.95.21	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
67.211.217.180	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
195.154.49.74	147.237.77.233	France	atal.idf.il	ET SCAN Potential SSH Scan	1
67.211.217.180	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
195.154.49.74	147.237.77.74	France	law.idf.il	ET SCAN Potential SSH Scan	1
195.154.49.74	147.237.76.34	France	yohalan.idf.il	ET SCAN Potential SSH Scan	1
195.154.49.74	147.237.8.46	France	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
13.92.139.45	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.8.28	France	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.0.35	France	akaws.idf.il	ET SCAN Potential SSH Scan	1
210.15.242.7	147.237.77.176	Australia	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.144.37	147.237.77.243	Switzerland	mobile.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.8.46	Latvia	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.77.243	France	mobile.idf.il	ET SCAN Potential SSH Scan	1
67.211.217.180	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
195.154.49.74	147.237.77.178	France	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
67.211.217.180	147.237.76.39	United States	mobile.meitav.idf.i	ET DROP Spamhaus DROP Listed Traffic Inbound	1
195.154.49.74	147.237.76.196	France	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.72.166	France	aka.idf.il	ET SCAN Potential SSH Scan	1
13.92.139.45	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
195.154.49.74	147.237.8.45	France	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
195.154.49.74	147.237.8.27	France	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
218.108.132.58	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.72.14	United States	dover.idf.il(old)	ET DROP Dshield Block Listed Source	1
195.216.176.244	147.237.8.14	Latvia	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

04-08-2016-01:08:24 to 04-08-2016-02:08:24

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10263
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	7562
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4046
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3237
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2644
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1252
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	955
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	356
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	255
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	195
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	179
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	drop		drop	164
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	drop		drop	96
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	82
37.110.98.20	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
176.77.57.36	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
176.77.90.222	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
93.80.66.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
176.77.57.22	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
141.0.14.145	Europe	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	19
141.0.14.145	Europe	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	16
2.54.191.114	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	15
41.200.146.242	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
160.162.154.224	Morocco	147.237.77.216	dover.idf.il	SYN Attack		reject	7
88.57.44.81	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
41.68.43.187	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.33.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.200.146.242	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.65.164.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
169.229.149.228	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
27.254.77.146	Thailand	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
169.229.149.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.111.165.15	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
160.162.154.224	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
190.34.149.226	Panama	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
2.54.148.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.217.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
177.13.33.19	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

04-08-2016-01:08:24 to 04-08-2016-02:08:24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.140.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.8.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
74.91.18.45	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.867bb.com/	Block	1
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
217.132.121.138	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/payslips.aspx	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.7.154.203	Japan	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
157.55.39.161	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1
66.249.79.178	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1926-he/cogat.aspx	Block	1
41.225.184.95	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/ui.datepicker.js	Block	1

04-08-2016-01:08:24 to 04-08-2016-02:08:24